CLAIMS

What is claimed is:

1. A method and system to deliver authentication authority Web services using non-reusable and non-reversible one-time identity codes, comprising:

(a) authentication authority means to serve as a powerhouse to authenticate user identity,

(b) gateway authority means to serve as a gateway to delegate said authentication authority Web services to said authentication authority means,

(c) authentication client means to serve as an end-user device to generate said one-time identity codes,

(d) authentication handler means to serve as a doorkeeper to protect resources of business entities using said authentication authority Web services,

(e) means comprising:

i. transmitting said one-time identity codes from said authentication client means to said authentication handler means,

ii. composing authentication requests by said authentication handler means, and transmitting said authentication requests from said authentication handler means to means selected from the group consisting of said gateway authority means and said authentication authority means.

iii. processing said authentication requests by said gateway authority means, and redirecting said authentication requests from said gateway authority means to said authentication authority means,

iv. generating authentication responses by said authentication authority means, and transmitting said authentication responses back to said authentication handler means,

whereby a scalable and distributable system to authenticate and validate said user identity will be provided,
whereby a user can use only a single said end-user device to generate said one-time identity codes to identify him/herself and to access protected resources of multiple said business entities,
whereby the authentication system can be used as an ID verification system for said business entities to verify said user identity over a channel selected from the group consisting of the Internet, phone and other communication means.

2. The method and system of claim 1 wherein said gateway authority means contain means to interact with other entities of said gateway authority means, and publish said authentication authority Web services to Web service industry's registries.

3. The method and system of claim 2 wherein said gateway authority means are arranged to use Web Services Description Language (WSDL) to publish said authentication authority Web services, and use Universal Description, Discovery and Integration (UDDI) standard to discover said authentication authority Web services published by other said gateway authority entities.

4. The method and system of claim 1 wherein said gateway authority means, said authentication authority means, said authentication handler means, and said authentication client means are arranged to use Simple Object Access Protocol (SOAP) to communicate, and use Hypertext Transport Protocol (HTTP) packets to transmit data over Secure Socket Layer (SSL).

5. The method and system of claim 4 wherein said data contains means to be transmitted by using File Transport Protocol (FTP) and Simple Mail Transport Protocol (SMTP).

6. The method and system of claim 1 wherein said gateway authority means and said authentication authority means contain means to be separated and placed in the Internet accessible environment to become said scalable and distributable system.

7. The method and system of claim 1 wherein said authentication authority means contain means to register and manage said user identity, said authentication client means identity, said user private identity, and associated vital information.

8. The method and system of claim 1 wherein said authentication authority means contain means for independently generating said one-time identity codes to authenticate said user identity.

9. The method and system of claim 1 wherein said authentication authority means contain means to use platforms which are vendor independent.

10. The method and system of claim 1 wherein said authentication responses generated by said authentication authority means contain means to inform said authentication handler said user identity.

11. The method and system of claim 1 wherein said authentication authority means and said authentication client means contain means to generate synchronization codes and conduct synchronization.

12. The method and system of claim 11 wherein said synchronization codes are arranged to be generated by math functions comprising hash, power and modular math operators, wherein said math functions are arranged to use said user identity, said authentication client identity, and said user private identity as the input information.

13. The method and system of claim 12 wherein said synchronization codes are arranged to contain limited information about said user identity, said authentication client identity, and said user private identity.

14. The method and system of claim 11 wherein said authentication authority means and said authentication client means contain means to generate confirmation codes to verify the success of said synchronization.

15. The method and system of claim 1 wherein said authentication authority means and said authentication client means contain means to independently generate non-predictable sequence number which is an essential part for producing said one-time identity codes.

16. The method and system of claim 15 wherein said non-predictable sequence number is arranged to be generated by math functions comprising hash, power and modular math operators, wherein said math functions are arranged to use said user identity, said authentication client identity, and said user private identity as the input information.

17. The method and system of claims 7, 12, 13 and 16 wherein said user private identity comprises said user's biometric identity and other shared secret information.

18. The method and system of claim1 wherein said authentication client means contain means to be incorporated in a portable, hand-held device.

19. The method and system of claim 1 wherein said authentication handler means is arranged to be executed on said business entities' computers.

20. The method and system of claim 1 wherein said authentication handler means contain means to receive and process said user logon request, compose and submit authentication request to said authentication authority means, process and validate returned authentication response from said authentication authority means, and grant permission for said user to log onto said business entities' computer.